Korean Patent Laid-Open No. 2001-0024179

Method and system for preventing illegal playback of digital data stream

Provided is a method and a system for preventing illegal playback of broadcasted digital data stream. The method includes a step of inserting a watermark in the digital data stream. The digital data stream including the inserted watermark is encoded. The encoded digital data stream is broadcasted with a ticket. The ticket and the encoded digital data stream are received. The encoded digital data stream is provided to a decoder in order to store the ticket and decode the digital data stream. The decoded digital data stream is received from the decoder. The watermark is extracted from the decoded digital data stream. A one-way encoding hashing function is applied to the stored ticket. The hashed ticket is compared to the extracted watermark. When the hashed watermark is not matched with the extracted watermark, the playback of the digital data stream is prevented.

[첨부그림 1]

특2001-0024179

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04N 5/913

(11) 공개번호 특2001-0024179
(43) 공개일자 2001년03월26일

(21) 출원번호 10-2000-7002950
(22) 출원일자 2000년03월20일
번역문제출일자 2000년03월20일
(86) 국제출원번호 PCT/EP1999/04773
(87) 국제공개번호 WO 2000/04713
(86) 국제출원출원일자 1999년07월07일
(87) 국제공개일자 2000년01월27일
(81) 지정국 EP 유럽특허 : 오스트리아 벨기에 스위스 독일 덴마크 스페인 프랑스 영국 그리스 아일랜드 이탈리아 룩셈부르크 모나코 네덜란드 포르투갈 스웨덴 핀랜드 사이프러스
국내특허 : 일본 대한민국 중국
(30) 우선권주장 60/093,402 1998년07월20일 미국(US)
09/323,608 1999년06월02일 미국(US)
(71) 출원인 코닌클리케 필립스 일렉트로닉스 엔.브이. 요트 게.아. 볼페즈
네덜란드왕국, 아인드호펜, 그로네보드스베그 1
(72) 발명자 엡스테인마렐 에이.
네덜란드왕국 아이아인드호펜5656 홀스트란6
파시에카미엘
네덜란드왕국 아이아인드호펜5656 홀스트란6
(74) 대리인 이병호

심사청구 없음

(54) 디지털 데이터 스트림 불법 재생 방지 방법 및 시스템

요약

방송된 디지털 데이터 스트림의 불법 재생을 방지하기 위한 방법 및 시스템이 제공된다. 이 방법은 디지털 데이터 스트림에 워터마크를 삽입하는 단계를 포함한다. 상기 삽입된 워터마크를 포함하는 상기 디지털 데이터 스트림이 암호화된다. 상기 암호화된 디지털 데이터 스트림이 티켓과 함께 방송된다. 상기 티켓 및 상기 암호화된 디지털 데이터 스트림이 수신된다. 상기 티켓을 저장하고 상기 디지털 데이터 스트림을 암호 해제하기 위해 상기 암호화된 디지털 데이터 스트림이 암호 해제 장치로 제공된다. 상기 암호 해제 장치로부터 상기 암호 해제된 디지털 데이터 스트림이 수신된다. 상기 암호 해제된 디지털 데이터 스트림으로부터 워터마크가 추출된다. 단일-방향 암호화 해싱 함수가 상기 저장된 티켓에 적용된다. 상기 해싱된 티켓이 상기 추출된 워터마크와 비교된다. 상기 해싱된 티켓이 상기 추출된 워터마크와 매칭되지 않을 때, 상기 디지털 데이터 스트림의 재생이 금지된다.

대표도

도3

색인어

워터마크, 해싱, 암호화, 티켓, 디지털 데이터 스트림

명세서

기술분야

본 발명은 일반적으로 방송 전송에 관한 것이고; 특히 방송된 디지털 데이터 스트림의 불법 재생을 방지하기 위한 방법 및 시스템에 관한 것이다.

배경기술

현재의 네트워크 환경에서 이러한 네트워크를 통해 분배될 수 있는 디지털 및 디지털화된 멀티 미디어 내용물의 확산으로 인하여, 저작권 보호가 핵심 논점이 된다. 저작권 보호는 저작권을 갖는 작품의 불법 복제의 확산을 방지 또는 금지하는 능력을 의미한다.

디지털 세계에서의 중요한 문제는 무제한적인 완전한 복제가 디지털 또는 디지털화된 내용물의 어떤 단편으로 부터도 만들어 질 수 있다는 것이다. 완전한 복제는 원본의 수정의 수의 스트림으로 구성된다면,

9-1

[첨부그림 2]

복제본도 그 스트림의 각 수에 대해 정확히 원본과 일치한다는 것을 의미한다. 그러므로, 복제를 하는 동안 원본 신호의 품질 저하가 없다. 아날로그 복제에서는 랜덤 노이즈가 항상 개입되어, 복제 신호의 품질을 저하시킨다.

소정의 내용물을 불법 복제하는 것은 디지털 또는 아날로그, 오디오, 비디오, 다른 것의 소프트웨어인지에 무관하게 일반적으로 해적 행위(저작권 침해)로 불린다. 해적 행위는 예를 들어, 그러한 불법 복제물을 판매하는 이익을 위해 또는, 그것에 대한 대가의 지불 없이 개인적인 사용을 위해 내용물의 복사본을 마련할 목적으로 행해진다. 해적 행위의 정의는 보호된 매체의 복사본이 이득 없이 분배되는 상황까지 확장되어왔다. 해적 행위의 문제는 디지털 내용물에 대해 가장 나쁘다. 이것은 해적이 일단 해적 행위를 방지하기 위해 구현되어 존재하는 어떤 보호 스킴을 파괴하는 방법을 발견하면, 그는 복사본의 품질 저하 없이 무제한적인 복사본을 만들 수 있기 때문이다. 반면에, 아날로그 세계에서는, 일반적으로 각각의 연속적인 복제의 내용물(신호)에 대한 품질 저하가 있으므로, 해적판의 양에 대한 일종의 자연적인 제한이 강제된다.

일반적으로, 저작권을 보호하기 위한 3가지 접근이 구현되어 왔다. 이것은 암호화(보안을 목적으로 데이터를 엔코딩하는 처리), 복사 방지 및, 내용물 확장이다. 복사 방지 및 내용물 확장은 일반적으로 디지털 세계에 적용되고, 일반적으로 스크램블링으로 불리는, 암호화에 관련된 스킴은 아날로그 신호에 적용된다. 이것은 보통 아날로그 케이블 시스템에서 발견된다.

암호화는 한번 암호화되면 그것이 암호 해제 또는 디스크램블될 때까지 사용할 수 없는 내용물을 스크램블한다. 예를 들어, 암호화된 비디오는 스크린 상에 랜덤 패턴으로 나타날 것이다. 암호화의 원리는 당신은 원하는 만큼의 복제본을 자유롭게 만들 수 있지만, 당신은 특수한 키를 사용하여 그것의 암호를 해제할 때까지는 응집된 어떤 것도 볼 수 없는 것이다. 이 키는 보호된 내용물에 대해 대가를 지불함으로써 얻을 수 있다. 그러나, 암호화 스킴은 부족함이 없는 것이 아니다. 예를 들어, 해적은 하나의 어떤 내용물의 암호화된 복사본을 살 수 있을 것이고, 이로써 암호 해제할 자격을 부여받는다. 그후, 해적은 암호 해제된 복제본의 무제한적인 복사를 할 수 있을 것이다.

복제 방지는 소프트웨어 기술자가 그것이 복제되었는지를 결정하고 만약 그렇게 되었다면 그것을 해산하도록 소프트웨어를 작성할 수 있는 다양한 방법을 포함한다. 그러나, 이 스킴은 그러한 방법이 역사적으로 회피되어왔기 때문에 상당히 포기되어왔다.

내용물 확장은 일부 여분의 정보를 복제본이 만들어 질 수 있는지의 여부를 나타내는 원본 내용물에 부가하는 어떤 시스템에 관한 것이다. 소프트웨어 또는 하드웨어 시스템은 이 부가적인 정보를 인식하고 적절한 방법으로 번역하기 위해 이러한 스킴의 범위에서 특별히 구축되어야한다. 그러한 소프트웨어 또는 하드웨어는 일반적으로 이러한 스킴에 "순응한다"라고 인용된다. 내용물 확장 시스템의 예는 Serial Copyright Management System embedded in Digital Audio Tape(DAT) hardware 이다. 이러한 시스템하에, 부가적인 정보는 복사 여부를 나타내는 오디오 내용물의 각각의 트랙에 선행하여 즉시 디스크 상에 저장된다. 하드웨어는 이 정보를 판독하고 사용은 이에 따른다.

내용물 확장 스킴에 부가된 것과 같은 정보는 워터마크의 사용을 통해 보호될 수 있는 내용물에 통합될 수 있다. 워터마크 아이디어에 대한 배경은 아이템들을 실질적으로 파괴하지 않고는 대응하는 아이템으로부터 제거될 수 없어야 한다는 것이다. 디지털 영역에서, 디지털 워터마크는 데이터에 영구히 삽입되어 어떠한 암호 해제 처리 후에도 데이터 내에 존재하는 지각할 수 없거나 양호하게 볼 수 없는 식별자 코드이다. 불행히도, 워터마크를 구현하는 저작권 보호 기술은 역사적으로 파괴되었다. 예를 들어, 워터마크를 구현하는 많은 기술들은 평균화로 불리는 기술에 의해 파괴되었다. 또한, 일부 워터마크 기술은 단순히 워터마크를 무시하여 파괴될 수 있다(즉, 워터마크 스킴에 순응하지 않음으로써).

위의 문제들은 디지털 장치의 확산에 의해 복잡해진다. 예를 들어, 아날로그 입력 신호를 수신하는 종래의 텔레비전에 비교하여 입력 디지털 신호의 재생이 가능한 디지털 텔레비전(예를 들어, 고 해상력 텔레비전(HDTV))들은 이제 개발되고 있고 사판되고 있다. 도 1은 종래 디지털 텔레비전(100)의 블록도이다. 텔레비전(100)은 수신기(102), 컨디셔널 엑세스(CA) 모듈(104), 및 수신기(102)와 CA 모듈(104)을 효과적으로 연결하는 버스(106)를 포함한다.

작동에 있어서, 신호는 안테나(108)를 통해 공중파로부터 축출되고 수신기(102)에 입력된다. 수신기(102)는 이 신호를 암호 해제하는 CA 모듈(104)로 보내고 암호 해제된 신호를 수신기(102)에 돌려보낸다. 버스(106)가 잠재적으로 탭될 수 있기 때문에, 비-순응 레코더/플레이어는 수신기(102)로 가장할 수 있고, 예를 들어 이 버스 상에 페이-퍼-뷰 프로그램(pay-per-view program)의 비트-포-비트 복사를 만들 수 있다. 그러므로, 비트-포-비트 복사는 신호가 CA 모듈(104)에 의해 암호 해제된 후 만들어 질 수 있다. 그러면, 비-순응 레코더/플레이어는 CA 모듈(104)로 가장할 수 있어서, 불법 복제된 프로그램은 수신기(102) 상에 디스플레이된다. 이러한 경우에, 수신기(102)는 암호 해제된 내용물을 (비-순응 레코더/플레이어에 의해) 받고, 이 내용물이 적법한 것으로 가정한다. 또한, 복제는 비-순응 재생 장치의 네트워크에 전송될 수 있다.

그러므로, 디지털 비디오 시스템과 같은 방송된 데이터 스트림의 불법 재생을 보호하기 위한 방법 및 시스템을 갖는 것이 매우 유리하고 바람직할 것이다.

발명의 상세한 설명

본 발명은 디지털 데이터 스트림의 불법 재생을 방지하기 위한 방법 및 시스템에 관한 것이다.

본 발명의 한 측면으로써, 디지털 데이터 스트림의 불법 재생을 방지하기 위한 방법은,

디지털 데이터 스트림에 워터마크를 삽입하는 단계,

상기 삽입된 워터마크를 포함하는 상기 디지털 데이터 스트림을 암호화하는 단계,

티켓과 함께 상기 암호화된 디지털 데이터 스트림을 방송하는 단계,

9-2

[첨부그림 3]

상기 티켓 및 상기 암호화된 디지털 데이터 스트림을 수신하는 단계;

상기 티켓을 저장하고, 상기 디지털 데이터 스트림을 암호 해제하기 위해 상기 암호화된 디지털 데이터 스트림을 암호 해제 장치로 제공하는 단계;

상기 암호 해제 장치로부터 상기 암호 해제된 디지털 데이터 스트림을 수신하는 단계;

상기 암호 해제된 디지털 데이터 스트림으로부터 워터마크를 추출하는 단계;

단일-방향 암호화 해싱 함수를 상기 저장된 티켓에 적용하는 단계;

상기 해싱된 티켓을 상기 추출된 워터마크와 비교하는 단계; 및

상기 해싱된 티켓이 상기 추출된 워터마크와 매칭되지 않을 때, 상기 디지털 데이터 스트림의 재생을 방지하는 단계를 포함한다.

본 발명의 다른 측면으로써, 방송된 디지털 데이터 스트림의 불법 재생을 방지하기 위한 시스템은,

버스;

암호화된 디지털 데이터 스트림을 암호 해제하기 위해 구성된 상기 버스에 효과적으로 결합된, 컨디셔널 엑세스 모듈;

삽입된 워터마크 및 티켓을 갖는 암호화된 디지털 데이터 스트림을 수신하기 위해 구성된 상기 버스에 효과적으로 결합되고, 상기 티켓을 저장하며, 상기 암호화된 디지털 데이터 스트림을 상기 컨디셔널 엑세스 모듈에 제공하며, 상기 컨디셔널 엑세스 모듈로부터 암호 해제된 디지털 데이터 스트림을 수신하는 수신기를 포함하며, 상기 수신기는,

상기 암호 해제된 디지털 데이터 스트림으로부터 상기 워터마크를 추출하기 위해 구성된 추출기;

상기 저장된 티켓에 단일-방향 암호화 해싱 함수를 제공하기 위해 구성된 해싱 모듈;

상기 해싱된 티켓을 상기 추출된 워터마크와 비교하기 위해 구성된 비교 모듈; 및

상기 해싱된 티켓이 상기 추출된 워터마크와 매칭되지 않을 때, 상기 디지털 데이터 스트림의 재생을 방지하기 위해 구성된 금지기를 포함한다.

본 발명의 이러한 측면, 특성 및 장점들은 첨부된 도면과 관련하여 읽혀질 뒤따르는 상세한 설명의 양호한 실시예로부터 명확해 질 것이다.

도면의 간단한 설명

도 1은 종래 디지털 텔레비젼의 블록도.

도 2는 본 발명의 실시예에 따른 디지털 데이터 스트림의 불법 재생을 방지하는 디지털 텔레비젼의 블록도.

도 3은 본 발명의 실시예에 따른 디지털 데이터 스트림의 불법 재생을 방지하는 방법을 도시하는 블록도.

실시예

본 발명은 예를 들어, 페이-퍼-뷰 프로그램과 같은 적법한 방송인 디지털 데이터 스트림의 불법 재생을 방지하기 위한 방법 및 시스템에 관한 것이다. 이것의 가장 근본적인 형식으로써, 예를 들어, 디지털 텔레비젼과 같은 재생 장치는 수신된 내용물의 저작권 상태를 점검하고 예를 들어, 불법 복제와 생방송이 아닌 것으로부터 불법적으로 얻어졌다고 결정되면 그러한 내용물에 대한 재생을 거절한다.

이러한 목적을 위해, 본 발명의 시스템과 방법은 디지털 워터마크 및 본 명세서에서 "티켓"으로 언급되는 참조 메커니즘에 의존한다. 디지털 워터마크 및 티켓은 다양한 복제 상태를 반영한다. 디지털 워터마크 또는 이 디지털 워터마크로 반영된 복제 방지 상태는 고정된다. 그러나, 티켓 또는 이 티켓으로 반영된 복제 방지 상태는 암호적으로 내용물을 처리(예를 들어, 재생, 기록, 또는 통과)와 관련된 내용물로 변경된다. 내용물이 재생되거나 기록되어야 할 때, 디지털 워터마크는 티켓에 비교된다. 티켓이 워터마크를 체크하면, 내용물은 복제 보호 상태에 따라 디스플레이되거나 기록될 수 있다. 그러나, 워터마크와 티켓이 서로 일치하지 않으면, 내용물은 디스플레이되지 않거나 기록되지 않는다.

디지털 워터마크 및 티켓을 사용하는 물리적 매체(예를 들어, 디지털 비디오 디스크(DVDs))를 위한 재생 제어 방법은 1997년 10월 16일에 Linnartz 등에 의한 "Philips Electronics Response to Call for Proposals Issued by the Data Hiding Subgroup Copy Protection Technical Working Group"의 논문에서 설명된다. 또한 Linnartz 논문은 디지털 데이터에 워터마크를 삽입하기 위한 두 가지 예시적인 방법을 설명한다. 이러한 두 가지 방법은 본 발명에 따라 디지털 데이터 스트림에 워터마크를 삽입하기 위해 사용될 수 있다.

제 1 방법은 디지털 데이터 스트림의 동영상 압축 처리 기술(MPEG) 코딩에 워터마크를 삽입한다. 제 2 방법은 디지털 데이터 스트림의 픽셀 데이터에 워터마크를 삽입한다. 그러나, 워터마크를 디지털 비디오 스트림에 삽입하기 위한 방법이 본 발명에서는 중요하지 않으므로, 위에 설명된 두 방법외의 방법들이 본 발명에 따라 사용될 수 있을 것이다. 따라서, 위의 두 방법 및 그들의 대응하는 장단점들은 본 명세서의 더욱 상세히 설명되지 않는다.

본 발명의 실시예에 따라 사용되는 복제 방지 상태가 table 1에 나타난다. 그러나, 본 발명은 이러한 복제 방지 상태 및 사용될 수 있는 다른 복제 방지 상태에 제한되지 않는다.

9-3

[청부그림 4]

표 1

복제 불가	내용물은 재생은 가능하나 복제는 불가
더 이상 복제 불가	내용물은 재생은 가능하나 복제는 불가
1회 복제 가	내용물은 재생 및 복제가 가능할 수 있으나, 복제본은 복제 불가 상태로 변경됨
복제 자유	내용물은 제한 없이 재생 및 복제 가능

위의 4개의 복제 방지 상태는 본 발명의 실시예에 따라 두 개의 워터마크 분류를 갖는다. 즉, 워터마크가 내용물을 "1회 복제 가" 또는 "더 이상 복제 금지"로 분류하거나, 워터마크가 내용물을 "복제 금지"로 분류한다. "1회 복제 가"와 "더 이상 복제 금지"와의 차이는 아래에서 설명될 티켓에 의해 만들어진다. "복제 자유"는 워터마크의 부재로 구현된다.

도 2는 본 발명의 실시예에 따른 예를 들어 디지털 비디오 스트림과 같은 디지털 데이터 스트림의 불법 재생을 방지하는 디지털 텔레비전의 블록도이다. 본 발명이 디지털 텔레비전을 인용하여 설명되는 동안, 예를 들어 디지털 비디오 또는 오디오 내용물과 같은 저작권있는 내용물의 불법 재생을 방지하기 위해 예를 들어, 아날로그 또는 디지털과 같은 어떤 재생 장치에 구현될 수 있다.

디지털 텔레비전(200)은 수신기(202), 컨디셔널 액세스(CA) 모듈(204), 및 수신기(202)와 CA 모듈(204)를 효과적으로 연결하는 버스(206)를 포함한다.

수신기(202)는 해싱 모듈(210), 추출기(212), 비교 모듈(214) 및 금지기(216)를 포함한다. 버스(205)는 도 1의 버스(106)와 동일하도록 한다. 실시예에 있어서, 수신기(202)는 안테나(218)를 통해 신호를 수신한다. 그러나, 안테나를 제외한 장치는 예를 들어, 위성 접시와 같은 것을 사용할 수 있다. 또한, 신호는 케이블 또는 다른 직접 전송 수단을 통해 수신기(202)에 직접 제공될 수 있다. 안테나(218)를 통해 신호를 수신하자마자, 수신기(202)는 이 신호를 암호 해제하는 CA 모듈(204)로 보내고 암호 해제된 신호를 수신기(202)에 돌려보낸다.

이러한 설명을 위해, 다음과 같이 가정된다. 즉, 수신기(202)는 순응한다(즉, 수신된 내용물(복제 방지 상태)에 허가를 부여하기 위한 법칙의 세트를 수여하고 워터마크를 판독할 수 있다.); CA 모듈(204)은 보안이 되어있다; 버스(206)는 보완이되어 있지 않다(예를 들어, 탭핑에 수반된다.).

위에서 언급된바와 같이, 버스(206)가 잠재적으로 탭될 수 있기 때문에, 비-순응 레코더/플레이어는 수신기(202)로 가장할 수 있고, 예를 들어 이 버스 상에 페이-퍼-뷰 프로그램(pay-per-view program)의 비트-포-비트 복사를 만들 수 있다. 그러므로, 비트-포-비트 복사는 신호가 CA 모듈(204)에 의해 암호 해제된 후 만들어 질 수 있다. 그러면, 비-순응 레코더/플레이어는 CA 모듈(204)로 가장할 수 있어서, 불법 복제된 프로그램은 수신기(202) 상에 디스플레이된다. 이러한 경우에, 수신기(202)는 암호 해제된 내용물을 (비-순응 레코더/플레이어에 의해) 받고, 이 내용물이 적법한 것으로 가정한다. 또한, 복제는 비-순응 재생 장치의 네트워크에 전송될 수 있다.

유리하게, 본 발명은 순응 수신기(202)가 생방송이 되지 않는 내용물을 받아들이는 실수를 방지하기 위해 참조 "티켓"을 제공한다. 도 3에는 이 티켓의 구현이 도시되고, 이것은 본 발명의 실시예에 따른 디지털 데이터 스트림의 불법 재생을 방지하기 위한 방법을 도시하는 블록도이다.

먼저, 워터마크가 보호되어야할 내용물에 삽입된다(단계 300). 워터마크는 내용물의 복제 방지 상태를 나타낸다. 도 3의 실시예에서, 내용물은 "복제 불가"로 워터마크된다.

그러면, 내용물(및 워터마크)은 암호화된다(단계 302). MPEG 비디오의 경우, 내용물(및 워터마크)를 포함하는 MPEG 전송 패킷들이 암호화된다. 그러면, 암호화된 내용물과 티켓이 방송된다(단계 304). MPEG 비디오의 경우, 티켓은 암호화되지 않은 사적인 MPEG 데이터로 보내진다.

내용물 및 티켓은 안테나(218)를 통해 공중파로부터 추출되고 텔레비전(200)의 수신기(202)로 입력된다(단계 306). 수신기(202)는 저장소(218)에 암호화되지 않은 티켓을 저장하고 암호화된 내용물은 CA 모듈(204)로 보낸다. 그러면, CA 모듈(106)은 내용물을 암호 해제하고 암호 해제된 내용물을 수신기(202)로 돌려보낸다(단계 308). 수신기(202)의 추출기(212)는 내용물로부터 워터마크를 추출한다(단계 310). 수신기(202)의 해싱 모듈(210)은 티켓에 단일 방향 암호화 해싱 함수를 두 번 적용한다. 단일 방향 암호화 해싱 함수는 텍스트 메시지로부터 고정 스트링 수를 발생하는 알고리즘이며, 이로 인해 이 고정된 스트링을 텍스트 메시지로 전환하는 것은 매우 어렵다. 예를 들어, M이 주어지면, h를 계산하는 것은 쉽다. h가 주어지면, M을 계산하기는 어렵고 H(M)=h이다. M이 주어지면 다른 메시지 N을 찾기가 어렵고 H(N)=H(M')이다. 단일 방향 해싱 함수의 더욱 상세한 설명을 위해, Bruce Schneier, John Wiley & Sons, Inc. (1996)의 "Applied Cryptography"를 참고할 수 있다. 그러면, 해싱된 티켓은 비교 모듈(214)에 의해 워터마크에 비교된다(단계 314). 해싱된 티켓과 워터마크가 매칭되면, 내용물은 디스플레이된다(단계 316). 반면에, 해싱된 티켓과 워터마크가 매칭되지 않으면, 금지기(216)는 내용물이 디스플레이되는 것을 방지한다(단계 318). 금지기(216)는 하드웨어 또는 소프트웨어(예를 들어, 비교 모듈(214)의 결과에 기초

9-4

[첨부그림 5]

하여 재생을 방지/허락하는 코드의 조각)로 구현될 수 있다.

금지기(216)는 수신기(202)가 비-순응 재생 장치에 의해 (CA 모듈(204)과 수신기(202) 사이의) 버스(206) 상에 놓이는 내용물이 디스플레이되는 것을 방지한다. 이 버스 상의 암호 해제된 내용물의 비-순응 재생은 CA 모듈(204)로부터 내용물을 수신하기 전에 오리지널로 방송된 디지털 비디오 스트림으로부터 티켓을 수신하지 않은 수신기(202)로 인해 실패한다. 수신기(202)가 티켓을 포함하지 않으므로, 추출된 워터마크의 체크는 수행되지 않는다. 또한, 워터마크가 내용물이 복제 금지를 나타내고, 티켓이 디지털 비디오 스트림의 오리지널 방송으로부터 저장되지 않았기 때문에, 수신기(202)는 내용물을 디스플레이하지 않는다.

다음의 명칭은 본 발명의 구현을 위해 사용된다.

P: 물리적 마크

T: 현재 상태의 티켓

W: 워터마크(또는 4회의 P 해싱)

물리적 마크의 설명이 이제 주어진다. 일반적으로, 예를 들어, 디지털 비디오 디스크(DVD)와 같은 물리적 매체에 저장된 디지털 정보는 최소한 ROM과 RAM 디스크를 구별하는 "물리적" 마크를 포함할 수 있다. 물리적 마크는 재생을 목적으로 하는 사용자가 활용할 수 없는 트랙에 적합할 수 있지만, 디스크(또는 특정 트랙(들))의 복제 방지 상태를 결정할 목적으로 사용하는 사용자만이 활용할 수 있다. 물리적 마크가 번호의 순서로 나타나므로, 방송된 디지털 비디오 스트림은, 번호의 순서를 구성하는 그들과 관련된 물리적 마크를 유사하게 가질 수 있다.

물리적 마크는 티켓을 발생하기 위해 사용된다. 즉, 티켓은 물리적 마크에 단일 방향 암호화 해싱 함수를 두 번 적용하여 얻어진다. 이것은 티켓이 비디오 스트림으로 방송됨에 따라 디지털 비디오 스트림을 방송하기에 앞서 이루어진다. 또한, 위에서 언급한 바와 같이, 티켓이 (수신기(202)에서) 워터마크에 비교되기 전에, 단일 방향 암호화 해싱 함수가 워터마크를 발생하기 위해 티켓에 두 번 적용된다. 이것은 T=H(H(P)), W=H(H(T))로 나타낼 수 있다.

해싱 함수가 위의 예에서 티켓에 두 번 적용되는 반면에, 해싱 함수는 워터마크를 발생하기 위해 티켓에 몇 번이든지 적용될 수 있다. 또한, 방송 스트림으로부터 얻어진 티켓은 선택적으로 파괴될 수 있다. 이것은 예를 들어, 카운트다운 카운터 또는 실시간 클락을 사용하여 소정의 주기 후에 이루어질 수 있다. 대안적으로, 티켓은 텔레비전의 전원이 오프된 후 파괴될 수 있다.

본 발명에 따른 (암호화) 참조 티켓의 사용은 디지털 데이터 스트림의 불법 재생을 방지하기 위한 상당히 안전한 방법을 제공한다. 그러므로, 응당한 대가를 지불한 사용자들에 제한된 서비스 및 프로그램의 재생이 제어될 수 있을 것이다. 그래서 그러한 프로그램 및 서비스의 해적 행위가 어려울 것이다. 또한, 해적 행위가 상당한 세입 손실을 가져오므로, 그러한 해적 행위를 방지하는 것은 상상컨대 이전에 해적판 내용물이 저 비용으로 정당한 소비자에게 제공되는 결과를 초래할 것이다.

비록 실시예가 첨부된 도면을 참고로 설명되었지만, 본 시스템 및 방법은 상세한 실시예에 국한되지 않고, 다양한 다른 변화 및 변경이 당업자에 의해 본 발명의 정신 및 범위를 벗어나지 않고 이루어질 수 있을 것이다. 그러한 모든 변화 및 변경은 첨부된 청구 범위에 의해 정의된 본 발명의 범위 내에 포함되도록 한다.

(57) 청구의 범위

청구항 1

디지털 데이터 스트림의 불법 재생을 방지하기 위한 방법에 있어서,

워터마크가 삽입된 암호화된 디지털 데이터 스트림을 티켓과 함께 방송하는 단계;

상기 티켓 및 상기 암호화된 디지털 데이터 스트림을 수신하는 단계;

상기 티켓을 저장하고 상기 디지털 데이터 스트림을 암호 해제하기 위해 상기 암호화된 디지털 데이터 스트림을 암호 해제 장치(204)로 제공하는 단계;

상기 암호 해제 장치(204)로부터 상기 암호 해제된 디지털 데이터 스트림을 수신하는 단계;

상기 암호 해제된 디지털 데이터 스트림으로부터 상기 워터마크를 추출하는 단계;

단일 방향 암호화 해싱 함수를 상기 저장된 티켓에 적용하는 단계;

상기 해싱된 티켓을 상기 추출된 워터마크와 비교하는 단계; 및

상기 해싱된 티켓이 상기 추출된 워터마크와 매칭되지 않을 때, 상기 디지털 데이터 스트림의 재생을 방지하는 단계를 포함하는 디지털 데이터 스트림 불법 재생 방지 방법.

청구항 2

디지털 데이터 스트림의 불법 재생을 방지하기 위한 방법에 있어서,

디지털 데이터 스트림에 워터마크를 삽입하는 단계;

상기 삽입된 워터마크를 포함하는 상기 디지털 데이터 스트림을 암호화하는 단계;

티켓과 함께 상기 암호화된 디지털 데이터 스트림을 방송하는 단계;

상기 티켓 및 상기 암호화된 디지털 데이터 스트림을 수신하는 단계;

9-5

[첨부그림 6]

상기 티켓을 저장하고 상기 디지털 데이터 스트림을 암호 해제하기 위해 상기 암호화된 디지털 데이터 스트림을 암호 해제 장치(204)로 제공하는 단계,

상기 암호 해제 장치(204)로부터 상기 암호 해제된 디지털 데이터 스트림을 수신하는 단계,

상기 암호 해제된 디지털 데이터 스트림으로부터 워터마크를 추출하는 단계,

단일 방향 암호화 해싱 함수를 상기 저장된 티켓에 적용하는 단계,

상기 해싱된 티켓을 상기 추출된 워터마크와 비교하는 단계, 및

상기 해싱된 티켓이 상기 추출된 워터마크와 매칭되지 않을 때, 상기 디지털 데이터 스트림의 재생을 방지하는 단계를 포함하는 디지털 데이터 스트림 불법 재생 방지 방법.

청구항 3

제 2항에 있어서,

상기 적용 단계는 1회 이상 수행되는 디지털 데이터 스트림 불법 재생 방지 방법.

청구항 4

제 2항에 있어서,

변호의 순서에 단일 방향 암호화 해싱 함수를 적용하여 상기 티켓을 발생하는 단계를 더 포함하는 디지털 데이터 스트림 불법 재생 방지 방법.

청구항 5

제 4항에 있어서,

상기 단일 방향 암호화 해싱 함수는 상기 변호의 순서에 1회 이상 적용되는 디지털 데이터 스트림 불법 재생 방지 방법.

청구항 6

제 2항에 있어서,

상기 해싱된 티켓이 상기 추출된 워터마크와 매칭되면, 상기 디지털 데이터 스트림의 재생을 허용하는 단계를 더 포함하는 디지털 데이터 스트림 불법 재생 방지 방법.

청구항 7

제 2항에 있어서,

상기 티켓을 파괴하는 단계를 더 포함하는 디지털 데이터 스트림 불법 재생 방지 방법.

청구항 8

방송된 디지털 데이터 스트림의 불법 재생을 방지하기 위한 시스템에 있어서,

버스(206),

암호화된 디지털 데이터 스트림을 암호 해제하기 위해 구성된 상기 버스에 효과적으로 결합된 컨디셔널 액세스 모듈(204),

삽입된 워터마크 및 티켓을 갖는 암호화된 디지털 데이터 스트림을 수신하기 위해 구성된 상기 버스(206)에 효과적으로 결합되고, 상기 티켓을 저장하며, 상기 암호화된 디지털 데이터 스트림을 상기 컨디셔널 액세스 모듈(204)에 제공하며, 상기 컨디셔널 액세스 모듈로부터 암호 해제된 디지털 데이터 스트림을 수신하는 수신기(202)를 포함하는 시스템으로서, 상기 수신기(202)는

상기 암호 해제된 디지털 데이터 스트림으로부터 상기 워터마크를 추출하기 위해 구성된 추출기(212),

상기 저장된 티켓에 단일-방향 암호화 해싱 함수를 제공하기 위해 구성된 해싱 모듈(210),

상기 해싱된 티켓을 상기 추출된 워터마크와 비교하기 위해 구성된 비교 모듈(214), 및

상기 해싱된 티켓이 상기 추출된 워터마크와 매칭되지 않을 때, 상기 디지털 데이터 스트림의 재생을 방지하기 위해 구성된 금지기(216)를 포함하는 디지털 데이터 스트림 불법 재생 방지 시스템.

청구항 9

제 8항에 있어서,

상기 해싱 모듈(210)은 상기 티켓에 단일 방향 암호화 해싱 함수를 1회 이상 적용하는 디지털 데이터 스트림 불법 재생 방지 시스템.

청구항 10

제 8항에 있어서,

상기 티켓은 전원 다운 모드에 진입하면 파괴되는 디지털 데이터 스트림 불법 재생 방지 시스템.

청구항 11

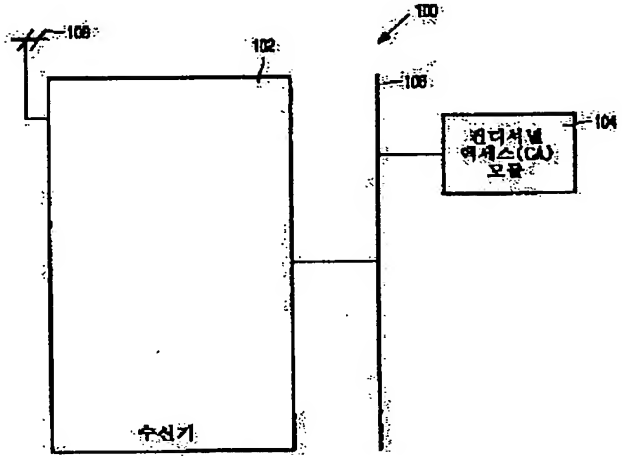
9-6

[첨부그림 7]

제 8항에 있어서,
상기 티켓은 소정의 시간 주기 후에 파괴되는 디지털 데이터 스트림 불법 재생 방지 시스템.

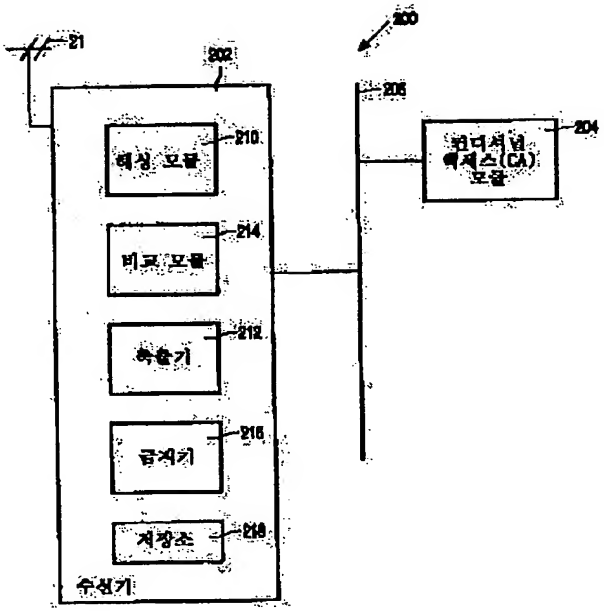
도면

도면1



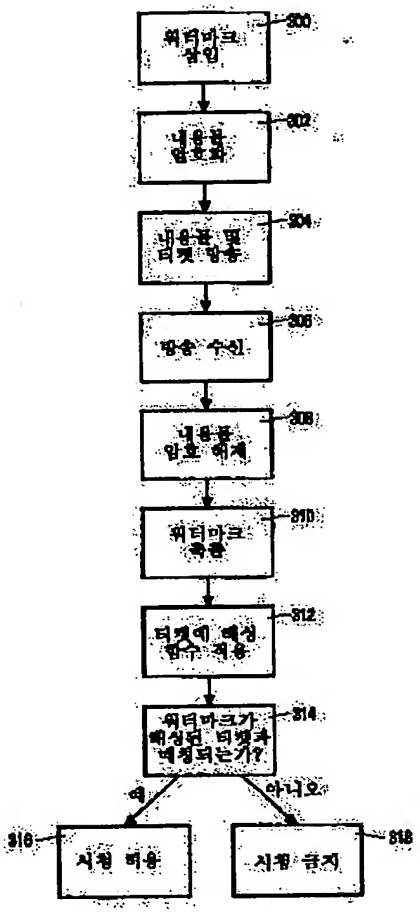
[첨부그림 8]

도면2


21
202
200
206
210
영상 모듈
204
커디셔널 액세스(CA) 모듈
214
비교 모듈
212
추출기
216
검지기
218
저장소
수신기

[첨부그림 9]

도면3


워터마크 삽입
300
내용물 압호화
302
내용물 및 티켓 방송
304
방송 수신
306
내용물 암호 해제
308
워터마크 추출
310
티켓에 해싱 함수 적용
312
워터마크가 해싱된 티켓과 매칭되는가?
314
예
아니오
시청 허용
316
시청 금지
318

9-9